



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/714,483

11/17/2003

Simon Charles Watt

550-471

6434

23117

7590

04/18/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER

JOHNSON, BRIAN P

ART UNIT

PAPER NUMBER

2183

DATE MAILED: 04/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/714,483

Applicant(s)

WATT ET AL.

Examiner

Brian P. Johnson

Art Unit

2183

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 17 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

1. Claims 1-39 have been examined.

Acknowledgment of papers filed: oath, specification, drawings, and IDS, on November 17th, 2003. The papers filed have been placed on record.

Specification

2. The title is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-16, 18, 20-34, 36 and 38-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Jackson (U.S. Publication No. 2002/0188831).
5. Regarding claim 1, Jackson discloses a method of controlling a monitoring function of a processor (paragraph 11, last 8 lines), said processor being operable in at

Art Unit: 2183

least two domains, comprising a first domain and a second domain (paragraph 11 lines 5-10), said first and second domains each comprising at least one mode (paragraph 11 lines 5-10),

Note that the two domains are considered to be distinguished by the trace enable bit. Also note that each of these two domains has one mode, one with traces and the other without.

Said method comprising the steps of: setting at least one control value (paragraph 11 line 7), said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain; and only allowing initiation of said monitoring function in said first domain when said condition is present (paragraph 62 col 2 lines 2-6) if its related control value indicates that said monitoring function is allowable.

6. Regarding claim 2, Jackson discloses a method according to claim 1, wherein said first domain is a secure domain and said second domain is a non-secure domain (paragraph 11 lines 5-10),

Note that the trace enable bit is considered to distinguish between a secure and non-secure domain. Once the trace has been enabled, trace information that was initially secure and unavailable will become non-secure and provided to the user for debugging purposes.

Said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data (paragraph 11

Art Unit: 2183

, last 8 lines.) which is not accessible when said processor is operating in a non-secure mode within said non-secure domain (paragraph 62, last 4 lines).

7. Regarding claim 3, Jackson discloses a method according to claim 2, wherein said condition comprises a domain, mode or type of monitoring function (paragraph 11 lines 5-10).

Note that the trace enable condition can be considered to be any one of a domain, mode or type of monitoring function.

8. Regarding claim 5, Jackson discloses a method according to claim 3, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode (paragraph 11 lines 5-10).

Note that the domain is considered to have one mode. Consequently, the mode for the secure domain is considered to be a secure user mode.

9. Regarding claim 6, Jackson discloses a method according to claim 5 wherein said control value comprises a secure user mode enable bit (paragraph 11 line 7) and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set (paragraph 62 col 2 lines 2-6).

10. Regarding claim 7, Jackson discloses a method according to claim 4, wherein said condition comprises a type of monitoring function (paragraph 62 lines 15-16).

Note that the trace annotation is considered to be the type of monitoring function.

11. Regarding claim 8, Jackson discloses a method according to claim 7, wherein said condition comprises a debug monitoring function (paragraph 11, last 8 lines) and said control value comprises a debug enable bit (paragraph 11 line 7), initiation of debug in said first domain only being allowable if said debug enable bit has been set (paragraph 62 col 2 lines 2-6).

Note that the debug enable bit is also considered to be the trace enable bit.

12. Regarding claim 9, Jackson discloses a method according to claim 8, wherein said condition comprises a trace monitoring function (paragraph 62 lines 15-16) and said control value comprises a trace enable bit (paragraph 11 line 7), initiation of trace in said first domain only being allowable if said control trace enable bit has been set (paragraph 62 col 2 lines 2-6).

13. Regarding claim 10, Jackson discloses a method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit (paragraph 11 line 7)

Note that these two bits are considered to be the same, so clearly one comprises the other.

And a secure trace enable bit (paragraph 11 line 7),

Again, the secure trace enable bit is considered to be the trace enable bit as well.

Initiation of debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set (paragraph 62 col 2 lines 2-6).

14. Regarding claim 11, Jackson discloses method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a different condition (paragraph 11 line 7 and paragraph 62 lines 15-20);

Note that the enable bit and the annotation instruction are considered to be two of the plurality of control values.

And only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control values related to a condition that is present indicate that said monitoring function is allowable (paragraph 62).

15. Regarding claim 12, Jackson discloses a method according to claim 1, said method further comprising said steps of: setting a control indicator (paragraph 11 line 7), said control indicator indicating that monitoring is only allowable for specified applications (paragraph 11 lines 5-10); and prior to initializing said monitoring function checking an application identifier; and only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable (paragraph 62 lines 15-20).

Note that the opcodes of the annotation instructions are considered to be application identifiers. The referenced invention only traces certain programs. Those programs are considered to be ones that include these particular annotation instructions. Recognition of these opcodes allows the processor to identify whether or not to save the trace for part of this application.

16. Regarding claim 13, Jackson discloses a method according to claim 12, wherein the step of setting a control indicator comprises setting a control indicator stored in a predetermined position in a storage element (fig 7 reference 702).

17. Regarding claim 14, Jackson discloses a method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data (paragraph 11, last 8 lines), said method comprising the further step of: following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain (paragraph 11 lines 5-10) while an application running on said processor is one for which monitoring is allowable (paragraph 62 lines 15-20).

18. Regarding claim 15, Jackson discloses a method according to claim 1, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data (paragraph 11, last 8 lines), said method comprising the further step of: following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain (paragraph 11 lines 5-10) when a condition changes if a control value

Art Unit: 2183

related to the changed condition indicates that said monitoring function is allowable (paragraph 62 col 2 lines 2-6).

19. Regarding claim 16, Jackson discloses a method according to claim 1, wherein setting of at least one control value is performed either by setting said control value via an input port (fig 7 reference 702 and col 11 line 7)

Note that the input port is considered to be the input wire for the register holding the enable bit.

Or by setting said control value from the first domain.

20. Regarding claim 18, Jackson discloses a method according to claim 1, wherein said first domain comprises a first user mode and a first privileged mode (paragraph 11 lines 5-10)

Note that the first domain is considered to be the first user mode and a first privileged mode.

And the step of setting at least one control value in said first domain, comprises setting said control value from said first privileged mode (paragraph 11 line 7).

21. Regarding claim 20, Jackson discloses a processor operable in a first domain and a second domain (paragraph 11 lines 5-10) said first and second domains each comprising at least one mode (paragraph 11 lines 5-10), said processor comprising: monitoring logic (fig 7 reference 730); a storage element operable to be set to contain at

Art Unit: 2183

least one control value (fig 7 reference 702), said at least one control value relating to a condition and being indicative of whether operation of said monitoring logic is allowable in said first domain (paragraph 11 lines 5-10); and control logic operable to control initiation of said monitoring logic (fig 7 reference 730 and paragraph 62 col 2 lines 2-6) and only to allow initiation of said monitoring logic in said first domain when said condition is present if its related control value indicates that operation of said monitoring logic is allowable (paragraph 62 col 2 lines 2-6).

22. Regarding claim 21, Jackson discloses a processor according to claim 20, wherein said first domain is a secure domain and said second domain is a non-secure domain (paragraph 11 lines 5-10)

Note: see claim 2.

Said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain (paragraph 62 col 2).

23. Regarding claim 22, Jackson discloses a processor according to claim 21, wherein said condition comprises a domain, mode or type of monitoring logic (paragraph 11 lines 5-10).

Note: see claim 3.

Art Unit: 2183

24. Regarding claim 23, Jackson discloses a processor according to claim 22, wherein said condition comprises a secure domain (paragraph 11 lines 5-10) and said control value comprises a secure domain enable bit (paragraph 11 line 7), initiation of monitoring in said secure domain only being allowed if said storage element contains a secure domain enable bit (paragraph 62 col 2 lines 2-6).

25. Regarding claim 24, Jackson discloses a processor according to claim 22, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode (paragraph 11 lines 5-10).

Note: see claim 5.

26. Regarding claim 25, Jackson discloses a processor according to claim 24 wherein said control value comprises a secure user mode enable bit (paragraph 11 line 7) and said control logic is operable to allow initiation of said monitoring logic from secure user mode only when said storage element contains a secure user mode enable bit (paragraph 62 col 2 lines 2-6).

27. Regarding claim 26, Jackson discloses a processor according to claim 21, wherein said condition comprises a type of monitoring function (paragraph 62 lines 15-16).

Note: see claim 7.

Art Unit: 2183

28. Regarding claim 27, Jackson discloses a processor according to claim 26, wherein said condition comprises debug monitoring (paragraph 11, last 8 lines) and the control value comprises a debug enable bit (paragraph 11 line 7), said control logic being operable to allow initiation of said monitoring logic in said first domain only when the storage element contains a debug enable bit (paragraph 62 col 2 lines 2-6).

Note: see claim 8.

29. Regarding claim 28, Jackson discloses a processor according to claim 26, wherein said condition comprises trace monitoring and said control value comprises a trace enable bit (paragraph 11 line 7), said control logic being operable to allow initiation of said trace logic in said first domain only when said storage element contains a control trace enable bit (paragraph 62 col 2 lines 2-6).

30. Regarding claim 29, Jackson discloses a processor according to claim 20, wherein: said storage element is operable to contain a plurality of control values, each of said plurality of control values relating to a different condition (paragraph 11 line 7 and paragraph 62 lines 15-20); and said control logic is operable to only allow initiation of said monitoring logic in said first domain if any of said conditions are present if each of the control values related to a condition that is present indicate that the monitoring logic is allowable (paragraph 62).

Note: see claim 11.

31. Regarding claim 30, Jackson discloses a processor according to claim 29 wherein one condition comprises a secure domain (paragraph 11 lines 5-10) and a corresponding control value comprises a secure domain enable bit (paragraph 11 line 7) and a further condition comprises a secure user mode (paragraph 11 lines 5-10) and a corresponding control value comprises a secure user mode enable bit (paragraph 11 line 7),

Note that the secure user mode and secure domain are considered to be the same mode.

Said control logic being operable to initiate said monitoring logic from secure user mode only when said storage element contains both a secure user mode enable bit and a secure domain enable bit (paragraph 11 lines 5-10).

Note that, clearly, the secure user mode will contain both of these bits since they are the same.

32. Regarding claim 31, Jackson discloses a processor according to claim 20, wherein: said storage element is further operable to contain a control indicator (paragraph 11 line 7), said control indicator indicating that monitoring is only allowable for identified applications (paragraph 11 lines 5-10); and said control logic is operable to check at least one identifier identifying an application that is allowable, said control logic only initiating said monitoring logic in the first domain when said application currently running is one identified as being one for which monitoring is allowable (paragraph 62 lines 15-20).

Note: see claim 12.

33. Regarding claim 32, Jackson discloses a processor according to claim 31, said processor comprising a further storage element, said storage element being operable to contain said at least one identifier specifying an application that is allowable (paragraph 62 lines 15-20).

Note that an indicator of which types of instructions are annotation instructions must be stored by the processor.

34. Regarding claim 33, Jackson discloses a processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data (paragraph 11, last 8 lines); and wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable (paragraph 62 lines 15-20).

35. Regarding claim 34, Jackson discloses a processor according to claim 20, said processor further comprising an input port, wherein said control value is operable to be set in said storage element either via the input port or via an input from said first domain (fig 7 reference 702 and col 11 line 7).

Note: see claim 16.

Art Unit: 2183

36. Regarding claim 36, Jackson discloses a processor according to claim 20, wherein said first domain comprises a first user mode and a first privileged mode (paragraph 11 lines 5-10) and said control value is operable to be set in said storage element via an input from said first privileged mode (paragraph 11 line 7).

Note: see claim 18.

37. Regarding claim 38, Jackson discloses a processor according to claim 20, wherein said storage element comprises a register (fig 7 reference 702).

Note that according to the American Heritage College dictionary, a computer science definition of a register is "a part of a central processing unit used as a storage location".

38. Regarding claim 39, Jackson discloses a processor according to claim 30, wherein said further storage element comprises a register (fig 7 reference 702).

Note: see claim 38.

39. Claims 1, 16, 17, 19, 20, 34, 35 and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by Dayan (U.S. patent No. 5,574,786).

Regarding claim 1 and 16, Dayan discloses a method of controlling a monitoring function (col 16 line 49) of a processor (col 4 line 25), said processor being operable in at least two domains (col 16 line 50), comprising a first domain and a second domain, said first and second domains each comprising at least one mode,

Note that the modes and the domains are considered to be one and the same, which means that each domain will comprise one mode.

said method comprising the steps of:

Setting at least one control value (col 6 lines 3-5),

Note that giving the user control to switch to a secure mode suggests the use of a control value indicating the current mode.

said at least one control value relating to a condition and being indicative of whether said monitoring function is allowable in said first domain (col 6 lines 15-20); and

Only allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable (col 16 lines 49-51),

Wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain (see below)

Note that both possibilities in the "or clause" are very broadly stated and considered anticipated by Dayan. In particular, an "input port" can consist of any port wire on the system computer that updates whatever bit value indicates whether the computer system is in a secure mode or not. Additionally, the control value can clearly be set from the first domain (secure domain); otherwise, there would be no way to go from a secure to an insecure domain.

Regarding claims 20 and 34, Dayan discloses a processor (col 4 line 25) operable in a first domain and a second domain said first and second domains each comprising at least one mode (col 16 line 50), said processor comprising:

Monitoring logic (col 16 lines 49-51);

Note that for the processing system to be able to complete a monitoring function, it clearly must also have logic to complete that functionality.

A storage element operable to be set to contain at least one control value (*note that the "control value" is considered to be the bit indicator of the secure/insecure mode*), said at least one control value relating to a condition and being indicative of whether operation of said monitoring logic is allowable in said first domain (col 16 lines 49-51); and

Control logic operable to control initiation of said monitoring logic and only to allow initiation of said monitoring logic in said first domain (col 16 lines 49-51) when said condition is present of its related control value indicates the operation of said monitoring logic is allowable (col 6 lines 3-5).

Wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain (see claims 1 and 16)

Regarding claims 17 and 35, Dayan discloses the method of claims 16 and 34, said method comprising the further step of blocking write access to said control value via said input port (col 16 lines 49-51) such that the step of setting said control value

can henceforth only be performed by setting said control value from said first domain (see below).

Note that 1) the blocking of the write access of the control value is done when there is no authentication code and 2) since the "control value" is considered to be the bit indicating the current mode of the computer system, clearly the only way to change the mode is to alter this control value.

Regarding claims 19 and 37, Dayan discloses the method of claims 16 and 34 wherein said first domain comprising a first user mode and a first privileged mode and said step of setting at least one control value in the first domain, comprises inputting an authentication code (col 4 lines 6-8) from a mode that is not a first privileged mode and then setting said control value (col 16 lines 49-51).

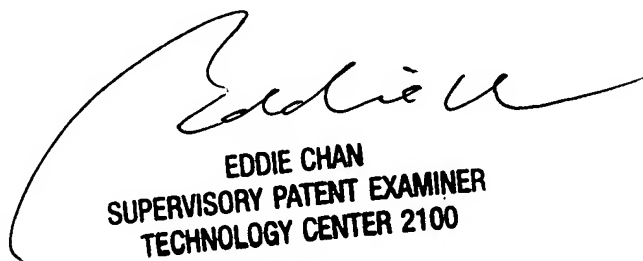
Conclusion

40. The following is text cited from 37 CFR 1.11(c): In amending in reply to a rejection of claims in an application or patent under reexamination, the applicant or patent owner must clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. The applicant or patent owner must also show how the amendments avoid such references or objections.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Johnson whose telephone number is (571) 272-2678. The examiner can normally be reached on 8-4:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eddie Chan can be reached on (571) 272-4162. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



EDDIE CHAN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100